

Application No.: 10/588,155
Inventor: KAGAYA
Docket No.: MIY.001.0045.PC

REMARKS/ARGUMENTS

Improper Final Rejection

Applicant respectfully requests that the finality of the Office Action of August 17, 2010 be withdrawn. The new grounds to reject independent claim 16 under 35 USC § 101 were not based on information submitted in an IDS filed during the period set forth in 37 C.F.R. §1.97(c), nor necessitated by an amendment of independent claim 16 – independent claim 16 was not amended in Applicant's reply of June 2, 2010. Accordingly, Applicant respectfully submits that the Office erred in making the Office Action of August 17, 2010 final and respectfully requests that the finality of the rejection be withdrawn.

Claim Amendments

Applicant has amended claims 1, 15 and 16 to include the limitations of claim 7, now canceled.

Claim Rejections under 35 USC § 101

Claim 16 was rejected as allegedly drawn to nonstatutory subject matter. Applicant has amended claim 16 to recite, in part, "a non-transitory computer readable medium including a computer program implementable on a computer to cause the computer," thereby rendering the rejection moot.

Withdrawal of the rejection is respectfully requested.

Claim Rejections under 35 USC § 102

Claims 1 – 16 stand rejected under 35 USC § 102 as allegedly anticipated by US 6,996,724 (Murakami). Applicant traverses the rejection in as much as it may apply to the claims as amended.

In accordance with the instant claims, random number partial data R(j) is generated from a random number in correspondence to original partial data S(j), and divided partial data D(i, j) is generated by using XOR calculation of the original partial data S(j) and the random number

Application No.: 10/588,155
Inventor: KAGAYA
Docket No.: MIY.001.0045.PC

partial data $R(j)$, and then as many divided data $D(i)$ as the desired number of divisions (n) are generated from the divided partial data $D(i, j)$.

The original partial data $S(j)$ is obtained by simply partitioning the secret information S by the prescribed processing unit bit length so that the secret information S can be reconstructed by concatenating the original partial data $S(j)$. However, the divided data $D(i)$ are n sets of data that are not obtained by partitioning the secret information S so that the secret information S cannot be reconstructed by simply concatenating the divided data $D(i)$. Rather, the divided data $D(i)$ can be reconstructed by concatenating the divided partial data $D(i, j)$, and the divided partial data $D(i, j)$ are obtained by using XOR calculation of the original partial data $S(j)$ and the random number partial data $R(j)$,

Here, the XOR calculation to be used in obtaining the divided partial data $D(i, j)$ is not mere calculation to take an XOR value of the original partial data $S(j)$ and the random number partial data $R(j)$. In other words, the divided data $D(i)$ and the divided partial data $D(i, j)$ are defined such that the secret information S can be recovered from a prescribed number of the divided data $D(i)$ but not from anyone divided data $n(i)$ alone as explicitly recited in claim 1.

By contrast, Murakami merely discloses a secret key generating method for generating a secret key of an entity in ID-NIKS (ID-based non-interactive key sharing scheme). In Murakami, the j -th center 1 extracts a row vector, which corresponds to the ID division vector of the entity a , from the symmetric matrix H_j and carries out XOR on all of the components of the extracted row vector with an individual random number $\alpha a(j)$ so as to be generated as a secret key vector S_{aj} , which is secretly distributed to the entity a . Additionally, in Murakami, the entity a extracts components, which correspond to the entity b , from the secret vectors received from respective J centers and those J components are synthesized through XOR so as to generate a common key K_{ab} for the entity b .

Murakami only discloses a method for generating a secret key and a common key and does not disclose a system for dividing secret information into divided data in a desired number of divisions as explicitly recited in claim 1.

Consequently, Applicant respectfully submits that Murakami fails to disclose the divided data $D(i)$ and the divided partial data $D(i, j)$ which is defined such that the divided data $D(i)$ can

Application No.: 10/588,155
Inventor: KAGAYA
Docket No.: MIY.001.0045.PC

be obtained by constructing the divided partial data $D(i, j)$, and the secret information S can be recovered from a prescribed number of the divided data $D(i)$ but not from anyone divided data $D(i)$ alone as explicitly recited in claim 1.

In addition to the above, Applicant respectfully submits that Murakami clearly fails to disclose the data re-division unit and the re-divided data storing unit as recited in claim 1.

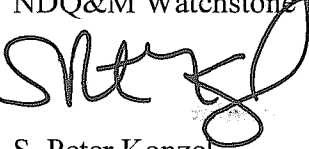
Finally, while the Office Action asserts that FIGS. 2-4 and Col. 6, line 26 - Col. 8, line 60 of Murakami teach and/or disclose various elements of Applicant's claims, the Office Action, however, fails to specifically show *how* the disclosure of Murakami teaches and/or discloses each and every element of Applicant's claims, as arranged – that is, the Office action merely recites Applicant's claims and, without any specificity, broadly asserts that such elements are disclosed by Murakami at FIGS. 2-4 and Col. 6, line 26 – Col. 8, line 60. In view thereof, Applicant respectfully requests that the Office, in the interest of compact prosecution, identify on the record and with sufficient specificity to support a *prima facie* case of anticipation, where in the Murakami reference each of the claim elements is alleged to be taught.

In view of the above, withdrawal of the rejection is respectfully requested.

Application No.: 10/588,155
Inventor: KAGAYA
Docket No.: MIY.001.0045.PC

Conclusion

Applicant respectfully submits that the present application is in condition for allowance, which action is courteously requested. Please charge any shortage in fees due in connection with the filing of this paper, including Extension of Time fees to Deposit Account No. 14-1437. Please credit any excess fees to such deposit account.

Respectfully submitted,
NDQ&M Watchstone LLP

S. Peter Konzel
Registration No.: 53,152

Customer No.: 58789
300 New Jersey Ave NW
5th Floor
Washington, D.C. 20001
Phone: (202) 659-0100
Fax: (202) 659-0105

Dated: November 17, 2010